PORTABLE TERMINAL AND PORTABLE TERMINAL INFORMATION PROTECTING METHOD

Patent Number:	JP9215057
Publication date:	1997-08-15
Inventor(s):	YAMAGUCHI MUNEAKI
Applicant(s):	HITACHI LTD
Requested Patent:	JP9215057
Application Number:	JP19960016402 19960201
Priority Number(s):	
IPC Classification:	H04Q7/38; G06F1/00; G09C1/00; H04L9/32; H04M3/42; H04M11/00
EC Classification:	
Equivalents:	

Abstract

PROBLEM TO BE SOLVED: To provide an information protection system and a portable terminal with which a terminal can be easily used at ordinary time and personal information left in the terminal can be protected and collected when the terminal is lost.
SOLUTION: According to a register request for information protection issued from a portable terminal 14, the security management data of the terminal 14 are registered in a security controller 10 connected to a radio network. When the terminal is lost and the owner of the portable terminal 14 requests the information protection to the security controller 10, an information protecting instruction is transmitted through the radio network to the portable terminal 14, and important information in the terminal is collected into the security controller 10 and made invalid by a dedicated program inside the portable terminal 14. Thus, even when the portable terminal 14 is lost, the important information can be collected and prevented from being abused.

JP Laid-open Publication No. Hei 9-215057 card

Portable Terminal and Portable Terminal Information Protecting Method

[0041]

At step 291, processing to protect confidentiality of terminal information (either invalidation or rewriting) is applied (291). Protection of data confidentiality is achieved, for example, by means of erasure of terminal information in a memory or conversion of the information to false data.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－215057

(43)公開日　平成９年(1997)８月15日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ			技術表示箇所
Ｈ０４Ｑ	7/38			Ｈ０４Ｂ	7/26	１０９Ｒ	
Ｇ０６Ｆ	1/00	３７０		Ｇ０６Ｆ	1/00	３７０Ｅ	
Ｇ０９Ｃ	1/00	６６０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６６０Ｄ	
Ｈ０４Ｌ	9/32			Ｈ０４Ｍ	3/42	Ｚ	
Ｈ０４Ｍ	3/42				11/00	３０２	

審査請求　未請求　請求項の数28　ＯＬ　（全 23 頁）　最終頁に続く

(21)出願番号　特願平8－16402

(22)出願日　平成８年(1996)２月１日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　山口　宗明
東京都国分寺市東恋ケ窪１丁目280番地
株式会社日立製作所中央研究所内

(74)代理人　弁理士　小川　勝男

(54)【発明の名称】　携帯端末および携帯端末情報保護方法

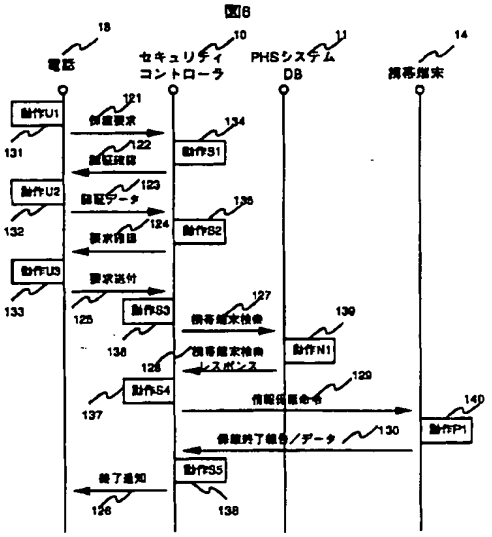
(57)【要約】

【課題】通常時の端末使用を容易にし、端末紛失時に端末内に残された個人情報の保護、回収を可能にした情報保護システムおよび携帯端末の提供。

【解決手段】携帯端末１４から発行した情報保護のための登録要求に従って、無線ネットワークに接続されたセキュリティコントローラ１０に、上記端末のセキュリティ管理データを登録しておく。端末紛失時に、携帯端末の所有者がセキュリティコントローラに情報保護を要求すると、無線ネットワークを通じて、当該携帯端末に情報保護命令が送信され、携帯端末内にある専用プログラムによって、端末内重要情報のセキュリティコントローラへの回収と無効化が行われる。

【効果】携帯端末が紛失しても重要情報を回収し、悪用を阻止できる。

図6



1

【特許請求の範囲】

【請求項1】無線通信手段と、出力手段と、入力手段と、ユーザデータを蓄積するためのメモリ手段と、上記入力手段からのユーザ操作入力に応じて、上記メモリ手段へのユーザデータの書込み、読み出し、上記出力手段への情報出力、および上記無線通信手段を介して他装置との情報の交信を行うためのデータ処理手段とからなる携帯端末装置において、

上記メモリ手段に記憶されているデータについての情報保護要求者を認証するための認証情報を記憶する手段と、

上記無線通信手段によって受信された情報保護命令メッセージに含まれる認証情報と上記記憶手段に予め記憶してある認証情報との対応関係から情報保護要求の正当性をチェックし、正当性が確認された場合に、上記メモリ手段に蓄積されている特定のユーザデータを無効化するための所定のデータ処理手順を記述した情報保護用ソフトウエアとを備え、

上記データ処理手段が、上記無線通信手段からの通知に応答して上記情報保護用ソフトウエアを実行し、上記特定のユーザデータを無効化して他人による利用を阻止するようにしたことを特徴とする携帯端末装置。

【請求項2】前記メモリ手段が、一般情報領域と保護情報領域とからなり、

前記データ処理手段が、上記情報保護用ソフトウエアを実行することにより、上記保護情報領域に蓄積されているユーザデータを無効化することを特徴とする請求項1に記載の携帯端末装置。

【請求項3】前記情報保護用ソフトウエアが、前記メモリ手段内に蓄積されている保護対象とすべきユーザデータのファイル識別情報を予め保持しており、

前記データ処理手段が、上記情報保護用ソフトウエアを実行することにより、上記ファイル識別情報で特定されたユーザデータを無効化することを特徴とする請求項1に記載の携帯端末装置。

【請求項4】前記情報保護用ソフトウエアが、ユーザデータ無効化に先立って、該当ユーザデータを前記情報保護命令メッセージの送信元に送信するための手順を含み、

前記データ処理手段が、上記情報保護用ソフトウエアを実行することにより、特定のユーザデータを他装置に回収した後、無効化することを特徴とする請求項1～請求項3の何れかに記載の携帯端末装置。

【請求項5】前記情報保護用ソフトウエアが、前記情報保護命令メッセージに含まれる処理区分コードに応じて、ユーザデータを無効化する前に、該ユーザデータを上記情報保護命令メッセージの送信元装置に選択的に送信するための手順を含み、

前記データ処理手段が、上記情報保護用ソフトウエアを実行することにより、上記ユーザデータを他装置に選択的に回収動作した後、無効化することを特徴とする請求項1～請求項3の何れかに記載の携帯端末装置。

2

【請求項6】前記情報保護用ソフトウエアが、データ消去によって前記ユーザデータを無効化させることを特徴とする請求項4または請求項5に記載の携帯端末装置。

【請求項7】前記情報保護用ソフトウエアが、データ変換によって前記ユーザデータを無効化させることを特徴とする請求項4または請求項5に記載の携帯端末装置。

【請求項8】前記情報保護要求メッセージの受信時に前記無線通信手段から出力される割込み信号に応答して、前記データ処理手段および前記メモリ手段の電源を自動的に投入動作する電源制御手段を備えたことを特徴とする請求項1～請求項7の何れかに記載の携帯端末装置。

【請求項9】携帯端末が保持しているユーザ情報の保護に必要なセキュリティ管理データをセキュリティ制御装置に登録するステップと、

携帯端末の所有者が、上記セキュリティ制御装置に対して、紛失状態にある携帯端末について情報保護を要求するステップと、

上記情報保護要求を受けたセキュリティ制御装置が、予め登録してあるセキュリティ管理データに基づいて情報保護命令メッセージを生成し、無線ネットワークを介して上記紛失状態にある携帯端末宛に送信するステップと、

上記情報保護メッセージを受信した携帯端末が、該端末内に保持する所定のユーザ情報について、他人による利用を阻止するためのデータ処理を施すステップとからなることを特徴とする携帯端末情報保護方法。

【請求項10】前記セキュリティ制御装置が、上記情報保護を要求された携帯端末について無線ネットワークによる通信が可能な状態にあるか否かをチェックし、通信可能な状態にあることを確認して、前記情報保護命令メッセージを送信することを特徴とする請求項9に記載の携帯端末情報保護方法。

【請求項11】前記セキュリティ制御装置が、上記情報保護を要求された携帯端末について無線ネットワークによる通信が可能な状態にあるか否かをチェックし、通信不能な状態にあった場合、上記携帯端末との無線通信可否を所定の繰返しパターンで繰り返すことを特徴とする請求項10に記載の携帯端末情報保護方法。

【請求項12】前記セキュリティ制御装置が、無線ネットワークに接続された移動端末データ管理装置に対して、前記情報保護を要求された携帯端末の状態を問合せ、

上記問合せを受けた移動端末データ管理装置が、上記携帯端末の位置登録の有無を上記セキュリティ制御装置に通知し、もし、現在位置が未登録状態にあった場合には、上記携帯端末について状態問合せを受けたことを記憶しておき、該当携帯端末が位置登録された時点で上記セキュリティ制御装置に通知し、

上記セキュリティ管理装置が、上記移動端末データ管理装置からの通知に応じて、前記情報保護命令メッセージを送信するようにしたことを特徴とする請求項９に記載の携帯端末情報保護方法。

【請求項１３】前記セキュリティ制御装置に登録されるセキュリティ管理データが、携帯端末のアドレス情報と、登録者識別情報と、登録者認証情報とを含み、
前記情報保護の要求時に、要求者が自分の識別情報と認証情報を提示し、上記セキュリティ制御装置が、上記提示された情報とセキュリティ管理データとして既に登録済の情報とに基づいて上記要求者の正当性をチェックし、正当性が確認された場合に、前記情報保護命令メッセージの生成と送信を行うことを特徴とする請求項９～請求項１２の何れかに記載の携帯端末情報保護方法。

【請求項１４】前記セキュリティ制御装置から送信される情報保護命令メッセージが前記認証情報を含み、
上記情報保護命令メッセージを受信した携帯端末が、該受信メッセージから抽出した認証情報と該携帯端末内に予め設定されている認証情報とに基づいて、上記受信メッセージの正当性をチェックし、正当性が確認された場合に、前記所定のユーザ情報について他人の利用を阻止するためのデータ処理を実行することを特徴とする請求項１３に記載の携帯端末情報保護方法。

【請求項１５】前記情報保護命令メッセージを受信した携帯端末が、予め指定してある所定のメモリ領域のユーザ情報について、他人の利用を阻止するためのデータ処理を施すことを特徴とする請求項９～請求項１４の何れかに記載の携帯端末情報保護方法。

【請求項１６】前記セキュリティ制御装置に登録されるセキュリティ管理データが、保護対象となる情報を特定するためのファイル識別情報を含み、前記セキュリティ制御装置が、前記情報保護命令メッセージ中に上記ファイル識別情報を設定し、
上記情報保護メッセージを受信した携帯端末が、受信メッセージ中のファイル識別情報で特定されたユーザ情報について、他人の利用を阻止するためのデータ処理を施すことを特徴とする請求項９～請求項１４の何れかに記載の携帯端末情報保護方法。

【請求項１７】前記情報保護命令メッセージを受信した携帯端末が、保護対象となった前記所定のユーザ情報を上記セキュリティ制御装置に送信した後、他人の利用を阻止するためのデータ処理を施すことを特徴とする請求項９～請求項１６の何れかに記載の携帯端末情報保護方法。

【請求項１８】前記情報保護命令メッセージを受信した携帯端末が、保護対象となった前記所定のユーザ情報を上記メッセージ中で指定された暗号鍵によって暗号化した形で上記セキュリティ制御装置に送信することを特徴とする請求項１７に記載の携帯端末情報保護方法。

【請求項１９】前記情報保護命令メッセージを受信した携帯端末が、保護対象となった前記所定のユーザ情報を消去することによって、他人の利用を阻止することを特徴とする請求項９～請求項１８の何れかに記載の携帯端末情報保護方法。

【請求項２０】前記情報保護命令メッセージを受信した携帯端末が、保護対象となった前記所定のユーザ情報にデータ変換を施すことによって、他人の利用を阻止することを特徴とする請求項９～請求項１８の何れかに記載の携帯端末情報保護方法。

【請求項２１】前記セキュリティ管理データの前記セキュリティ制御装置への登録が、保護対象となる携帯端末から無線ネットワークを介して行われることを特徴とする請求項９～請求項２０の何れかに記載の携帯端末情報保護方法。

【請求項２２】前記セキュリティ制御装置への情報保護要求が、電話を利用して行われることを特徴とする請求項９～請求項２１の何れかに記載の携帯端末情報保護方法。

【請求項２３】携帯端末と、無線ネットワークと、上記無線ネットワークに接続されたセキュリティ制御装置とからなり、
上記セキュリティ制御装置が、携帯端末に関するセキュリティ管理データを記憶するための記憶手段と、紛失状態にある携帯端末の所有者からのデータ保護要求に応じて、上記セキュリティ管理データに基づいてデータ保護命令メッセージを生成し、これを上記無線ネットワークを介して該当携帯端末に送信するためのメッセージ生成送信手段を備え、
上記セキュリティ制御装置にセキュリティ管理データを登録済の携帯端末が、上記無線ネットワークと通信するための無線通信手段と、データ処理手段と、上記無線通信手段で受信したデータ保護命令メッセージに応答して上記データ処理手段によって実行すべき専用ソフトウエアとを備え、上記専用ソフトウエアの実行によって、上記携帯端末内の特定のデータを無効化するようにしたことを特徴とする携帯端末の情報保護システム。

【請求項２４】前記セキュリティ制御装置が、前記携帯端末所有者からのデータ保護要求時に、上記所有者が提示した個人認証情報と前記セキュリティ管理データとして予め登録されている個人認証情報とに基づいて上記保護要求の受け付け可否を判定する判定手段を備え、受付可と判断されたデータ保護要求について前記データ保護命令メッセージの生成と送信を行うことを特徴とする請求項２３に記載の携帯端末の情報保護システム。

【請求項２５】前記セキュリティ制御装置のメッセージ生成送信手段が、前記データ保護命令メッセージ中に前記セキュリティ管理データで予め登録されている個人認証情報を含めた形でメッセージを送信し、
前記携帯端末が、受信したデータ保護命令メッセージに含まれる個人認証情報と予め該携帯端末に記憶されてい

る個人認証情報とに基づいて、上記データ保護命令メッセージへの応答可否を判定する判定手段を備え、
上記判定手段で応答可と判断されたデータ保護命令メッセージに応答して、前記特定のデータについてのデータ処理を実行するようにしたことを特徴とする請求項２３または請求項２４に記載の携帯端末の情報保護システム。

【請求項２６】前記携帯端末の無線通信手段が、前記データ保護命令メッセージを識別し、前記データ処理手段の電源を自動的に投入するための電源制御手段を備えることを特徴とする請求項２３～請求項２５の何れかに記載の携帯端末の情報保護システム。

【請求項２７】前記携帯端末の専用ソフトウエアが、前記特定のデータについて、前記セキュリティ制御装置に転送した後、データ消去またはデータ暗号化によって他人に対するデータ無効化を行うことを特徴とする請求項２３～請求項２６の何れかに記載の携帯端末の情報保護システム。

【請求項２８】前記携帯端末が、前記セキュリティ制御装置への転送データを暗号化するための手段を備えることを特徴とする請求項２７に記載の携帯端末の情報保護システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、携帯端末および携帯端末情報保護方法に関し、更に詳しくは、マイクロプロセッサとメモリ手段と無線通信手段とを備えた可搬型端末、およびメモリに蓄積されたユーザ情報の保護方法に関するのものである。

【０００２】

【従来の技術】半導体メモリやマイクロプロセッサ等の電子技術の向上によって、ノート型のパーソナルコンピュータの他に、電子手帳、パーソナルデジタルアシスタンツ（Personal Digital Assistants：ＰＤＡ）、新携帯情報ツールなどと呼ばれる携帯端末装置が実用化されている。特に小型化、軽量化された携帯端末装置は、上着のポケットなどに入れて容易に持ち運ぶことができ、移動途中でデータの入出力操作をしたり、通信機能を利用して出先からオフィス側の情報処理システムとデータ交信する等、利用形態も多様化している。

【０００３】然るに、これらの携帯端末装置は、所有者本人によってオフィス外に持ち出され、また、鞄やポケット等に入れ持ち運ばれるため、移動途中で盗難に遭遇したり、不注意による紛失、置き忘れ等、本人の意に反した形で他人の手に渡る機会が増え、端末装置内に記憶された情報が第三者に参照、悪用される危険性が高まってきている。従来、秘密性の高い情報を保護するための方法として、アクセスを制限すべき情報ファイルにはパスワードを対応付けておき、利用者がこの情報ファイルを参照しようとすると、システム側からパスワードの入力を促し、入力されたパスワードが予め登録されている正規のものと一致した場合にのみ、アクセスを許容する方法が知られている。

【０００４】

【発明が解決しようとする課題】携帯端末は、主として個人の所有物として利用され、オフィス内に設置された固定端末のように不特定の複数の利用者が共用したり、他人に貸し借りすることを前提としたものではない。このため、携帯端末の所有者は、端末が自分の管理下にある間は、携帯端末内にあるユーザ情報の保護について意識することは稀である。また、携帯端末の所有者は、携帯端末の蓄積情報を自分の所有物として気軽に扱うことを望み、他人に見られてはならない情報であっても、平常時には、手続き的に面倒な上述したパスワード等による秘密保護策はとらず、必要な情報を随時、迅速にアクセスできる操作環境で端末を利用することが多い。携帯端末の所有者が、端末内の蓄積情報について他人による参照と利用を是非とも避けたいと意識するのは、自分の端末が紛失したことに気付いた時である。

【０００５】本発明の目的は、端末を紛失した時、該端末内に残された所有者にとって重要な情報が第三者に悪用されるのを防止できるようにした携帯端末装置、端末情報の保護方法および端末情報保護システムを提供することにある。本発明の他の目的は、端末を紛失した時、該端末内に残された所有者にとって重要なユーザ情報を所有者の手元に回収できるようにした携帯端末装置、端末情報の保護方法および端末情報保護システムを提供することにある。本発明のさらに他の目的は、通常時において端末内の蓄積情報へのアクセスが容易であり、端末紛失時に該端末内に残された所有者にとって重要なユーザ情報を保護できるようにした携帯端末装置、端末情報の保護方法および端末情報保護システムを提供することにある。

【０００６】

【課題を解決するための手段】上記目的を達成するため、本発明の携帯端末情報保護方法および保護システムでは、携帯端末に格納されているユーザ情報を保護するために必要なセキュリティ管理データを無線ネットワークに接続されたセキュリティ制御装置に予め登録しておき、携帯端末の紛失に気付いた端末所有者が、上記セキュリティ制御装置に対して自分の携帯端末についての情報保護を要求すると、セキュリティ制御装置が、予め登録してあるセキュリティ管理データに基づいて情報保護命令メッセージを生成し、これを無線ネットワークを介して携帯端末に送信し、上記情報保護メッセージを受信した携帯端末が、端末内に保持する所定のユーザ情報について他人の利用を阻止するためのデータ処理を施すようにしたことを特徴とする。

【０００７】本発明の実施例によれば、上記セキュリティ制御装置が、目的の携帯端末が無線ネットワークによ

る通信が可能な状態にあるか否かをチェックし、通信可能な状態にあることを確認して上記情報保護命令メッセージを送信し、もし通信不能な状態であれば、通信可否の確認を所定の繰返しパターンで繰り返すようにしている。上記情報保護命令メッセージの送信に先立って、上記セキュリティ制御装置が、無線ネットワークにおける移動端末データを管理する管理装置に対して目的携帯端末の状態を問合せ、上記移動端末データ管理装置が、セキュリティ制御装置に上記携帯端末の位置登録の有無を通知し、もし、位置登録されていなかった場合には、上記携帯端末について状態問合せを受けたことを記憶しておき、当該携帯端末が位置登録された時点で上記セキュリティ制御装置に通知するようにし、上記セキュリティ管理装置が、移動端末データ管理装置からの通知に応じて情報保護命令メッセージを送信するようにしてもよい。

【０００８】本発明において、上記セキュリティ管理データは、例えば、携帯端末のアドレス情報（無線ネットワークにおけるアドレスまたは電話番号）と、登録者識別情報と、登録者認証情報と含む。このような管理データを予めセキュリティ制御装置に登録しておくことによって、情報保護の要求時に、要求者（紛失した携帯端末の所有者）に自分の識別情報と認証情報を提示させ、セキュリティ制御装置が、上記提示された情報と、セキュリティ管理データとして既に登録済の情報とを照合して要求者の正当性をチェックし、正当性が確認された場合に限り、上記情報保護命令メッセージの生成と送信を行わせるようにすることができる。また、携帯端末に送信する情報保護命令メッセージに上記認証情報を設定しておき、上記情報保護命令メッセージを受信した携帯端末に、受信メッセージから抽出した認証情報と携帯端末内に予め設定されている認証情報とに基づいて上記受信メッセージの正当性をチェックさせ、正当性が確認された場合に限り、情報保護のためのデータ処理を実行させることができる。

【０００９】本発明による携帯端末は、無線通信手段と、出力手段と、入力手段と、ユーザデータを蓄積するためのメモリ手段と、上記入力手段からのユーザ操作入力に応じて、上記メモリ手段へのユーザデータの書込み、読み出し、上記出力手段への情報出力、および上記無線通信手段を介して他装置との情報の交信を行うためのデータ処理手段とからなる携帯端末装置において、上記メモリ手段に記憶されているデータについての情報保護要求者を認証するための認証情報を記憶する手段と、上記無線通信手段によって受信された情報保護命令メッセージに含まれる認証情報と上記記憶手段に予め記憶してある認証情報との対応関係から情報保護要求の正当性をチェックし、正当性が確認された場合に、上記メモリ手段に蓄積されている特定のユーザデータを無効化するための所定のデータ処理手順を記述した情報保護用ソフトウエアとを備え、上記データ処理手段が、上記無線通信手段からの通知に応答して上記情報保護用ソフトウエアを実行し、上記特定のユーザデータを無効化して他人による利用を阻止するようにしたことを特徴とする。

【００１０】保護すべきユーザデータを特定するために、本発明の携帯端末では、例えば、メモリ手段を一般情報領域と保護情報領域とに分けておき、情報保護上記保護情報領域に蓄積されているユーザデータについて無効化する。この代わりに、情報保護用ソフトウエアが、保護対象とすべきユーザデータのファイル識別情報を予め保持し、上記ファイル識別情報で特定されたユーザデータを無効化するようにしてもよい。ユーザデータの保護形態として、上記情報保護用ソフトウエアにより、ユーザデータ無効化に先立って、ユーザデータを他の装置、例えば、上記情報保護要求メッセージの送信元に転送し、後で端末所有者の手元に回収できるようにしてもよい。この場合、上記ユーザデータを暗号化して転送するようにしてもよい。

【００１１】

【発明の実施の形態】図１は、無線ネットワークを利用した本発明による携帯端末情報の保護方法を実現するためのシステム全体構成を示す。図において、１は、有線網５を介して相互接続された複数の無線基地局１２（１２Ａ～１２Ｎ）と移動端末制御データを格納したデータベースシステム１１とからなる無線ネットワーク、１０は上記無線ネットワークに接続されたセキュリティコントローラ（セキュリティサーバ）である。１４（１４Ａ～１４Ｍ）は上記無線ネットワークを利用する移動端末であり、通常の移動電話機の他に、本発明が対象とする携帯情報端末（以下、単に携帯端末という）もこれらの移動端末の一種となる。以下の実施例では、無線ネットワーク１としてＰＨＳ(Personal Handy-phoneSystem)を適用した場合について説明する。有線網５には、図示しない交換機システムを介して、固定端末１８や他の公衆電話通信網が接続される。但し、上記無線ネットワーク１には、携帯端末とセキュリティコントローラとの間で計算機コマンドおよびデータを含むメッセージの通信を可能とする他の方式のものを適用してもかまわない。

【００１２】上記データベースシステム（ＰＨＳシステムＤＢ）１１には、移動端末制御データとして、移動端末（ＰＨＳ電話機およびＰＨＳ機能内蔵の携帯端末）の位置情報や認証情報などが管理され、本実施例では、セキュリティコントローラ１０は上記データベースシステムと結合されている。セキュリティコントローラ１０は、携帯端末１４の所有者からのセキュリティ登録要求に応じて、携帯端末１４の情報保護に必要なセキュリティ管理データを登録しておき、電話１８等の通信装置を介してユーザから携帯端末情報の保護要求を受けたとき、予め登録されているセキュリティ管理データに基づいて、ユーザの認証、携帯端末の特定を行い、無線ネッ

トワークシステムを介して、後述する目的端末の現在位置情報の入手と情報の保護動作を行う。携帯端末１４の位置情報は、ＰＨＳシステムＤＢ１１をアクセスすることにより得られ、情報保護は、携帯端末１４に情報保護命令を送信し、携帯端末に内蔵されている情報保護プログラムを実行させることにより実現する。

【００１３】図２は、携帯端末の所有者によるセキュリティコントローラ１０への情報保護登録の手順を示す。携帯端末１４で登録操作５７を行うと、セキュリティコントローラ１０と接続され、セキュリティコントローラ１０に登録要求５１が送信される。セキュリティコントローラ１０は、上記登録要求５１に応答して登録受付動作６１を実行し、要求元の携帯端末１４に登録情報要求５２を送付する。携帯端末１４は、上記登録情報要求に応じて、所有者に情報保護に必要な情報を入力させ、これを登録情報５３としてセキュリティコントローラ１０に送信する。セキュリティコントローラ１０は、上記登録情報５３を解析した後、登録情報確認要求５４を携帯端末４に送信する。所有者が、登録内容に誤りのないことを確認すると、登録確認応答５５が携帯端末１４からセキュリティコントローラ１０に送付される。セキュリティコントローラ１０は、上記登録確認応答を受信すると、登録情報確認動作６３を実行し、登録情報５３を登録データテーブルに登録し、携帯端末１４に登録ＯＫレスポンス５６を送信して登録処理を終了する。同様に、携帯端末側でも、上記登録ＯＫレスポンス５６を受信し、これをユーザが確認して登録処理を終了する。

【００１４】図３は、携帯端末とセキュリティコントローラとの間で通信される携帯端末情報保護用のメッセージフォーマット７０を示す。メッセージ７０は、システムＩＤ７１、動作ＩＤ７２、データ量７３、データ内容７４、およびＣＲＣ（サイクリック・リダンダンシー・チェック）７５の５つのフィールドからなる。システムＩＤ７１には、このメッセージが携帯端末情報保護用のものであることを示すコードが設定される。動作ＩＤ７２は、このメッセージの種類を示し、登録要求５１、登録情報要求５２等を識別するための識別子が設定される。データ量７３は、後続するデータ内容フィールド７４のデータ量をバイト単位で示し、ＣＲＣ７５は、動作ＩＤフィールド７２からデータ内容フィールド７４までのデータ誤りチェックに利用される。

【００１５】登録要求５１に応答してセキュリティコントローラ１０から携帯端末に送信される登録情報要求メッセージ５２のデータ内容７４は、データフォーマット７６で示すように、必要データひな型７９と暗号鍵Ａ：８０とを含む。必要データひな型７９は、登録情報５３として必要な情報項目を携帯端末所有者に表示するためのデータであり、入力すべき情報項目を表す文字列とそのバイト長とで構成されている。暗号鍵Ａ：８０は、例えば、公開暗号鍵方式における公開暗号鍵であり、携帯端末１４は、登録情報５３を上記暗号鍵Ａを用いて暗号化した形で、セキュリティコントローラに送信する。

【００１６】登録情報メッセージ５３のデータ内容７４は、データフォーマット７７で示すように、携帯端末識別ＩＤ８１、携帯端末電話番号８２、登録者ＩＤ８３、認証情報８４、処理番号８５、および暗号鍵Ｂ：８６を含む。携帯端末識別ＩＤ８１は、携帯端末のシリアルナンバーであり、セキュリティコントローラが携帯端末と通信する際に、正しい携帯端末と通信しているか否かの判定に用いられる。携帯端末電話番号８２は、携帯端末が内蔵するＰＨＳの電話番号であり、セキュリティコントローラ１０は、この電話番号によって、紛失状態にある携帯端末を呼び出す。登録者ＩＤ８３は、携帯端末所有者のＩＤであり、セキュリティコントローラは、携帯端末情報保護サービスの実行に際して、このＩＤで利用者とセキュリティ管理データを特定する。認証情報８４は、携帯端末情報保護サービスの要求者が登録者本人か否かを確認するための暗証情報（パスワード）である。処理番号８５は、端末情報保護の形態を示す。例えば、端末が保持する情報（保護情報）を消去する場合は「処理番号＝１」、保護情報をセキュリティコントローラ側に回収（転送）した後、端末の保持する情報を消去する場合は「処理番号＝２」、の如く端末情報保護の形態（種類）をコード化しておき、端末所有者は、登録時に予め情報保護の形態を指定しておく。暗号鍵Ｂ：８６は、公開暗号鍵方式の公開暗号鍵であり、セキュリティコントローラから携帯端末に送信する情報を暗号化するために用いられる。

【００１７】登録ＯＫレスポンス５６のデータ内容７４は、データフォーマット７８に示すように、登録者ＩＤ８３と処理番号８５を含む。処理番号８５は、上記登録情報メッセージ５３において利用者が指定し、セキュリティコントローラ側で受け付けられた処理番号を示す。

【００１８】図４は、登録手続きのために携帯端末に表示されるデータ入力画面の１例を示す。９０は登録開始画面、９１は登録情報入力画面、９２は所有者確認画面であり、端末所有者は、表示内容に従って順次にデータを入力する。登録開始画面９０において、メニュー９３から「セキュリティ登録」を選択すると、登録ウィンドウ９４が表示される。登録ウィンドウ９４には、端末紛失時の情報保護を要求するとき使用する非常時連絡先電話番号と、情報登録処理の実行要否を指示するための「ＹＥＳ（はい）」、「ＮＯ（いいえ）」のボタンが用意されている。情報登録処理を実行しようとする端末所有者は、上記非常時連絡先電話番号を手帳等にメモした後、「ＹＥＳ（はい）」ボタンを選択する。この操作によって、携帯端末からセキュリティコントローラ１０へ自動的にダイヤルされ、コネクションが確立されると、携帯端末からセキュリティコントローラ１０に登録要求５１が送信される。なお、上記自動ダイヤルされる電話

番号は、上記非常時連絡先電話番号とは別のものとする。また、上記非常時連絡先電話番号は、携帯端末にロードされる情報保護用のソフトウエアの説明書で確認するようにしてもよい。

【００１９】登録情報入力画面９１は、登録情報要求メッセージ５２でセキュリティコントローラ１０から送信された必要データひな形７９に基づいて構成される登録情報入力ウィンドウ９５を有し、端末所有者は、このウィンドウで登録情報（セキュリティ管理データレコード）として必要な複数項目のデータを入力する。全てのデータ項目の入力を終え、所有者が送信ボタンを選択すると、データ内容７４としてデータフォーマット７７の内容をもつ登録情報メッセージ５３が生成され、セキュリティコントローラ１０に送付される。ユーザ確認画面９２は、セキュリティコントローラ１０から登録ＯＫレスポンス５６を受信した時、携帯端末に表示される画面であり、終了ボタンと登録情報を含むユーザ確認ウィンドウ９６が表示される。所有者が、終了ボタンを選択すると登録処理が終了する。このとき、セキュリティ管理データの一部、例えば、登録者ＩＤとパスワードは、携帯端末内の不揮発性メモリに記憶保持される。

【００２０】図５は、登録処理時にセキュリティコントローラ１０が実行する処理プログラムのフローチャートの１例を示す。ブロック６１、６２、６３は、それぞれ図２に示した登録受付動作６１、登録情報受付動作６２、登録情報確認動作６３に対応している。セキュリティコントローラ１０は、携帯端末からの着信待ち状態（ステップ１０１）にあり、着信がなければ、常駐処理（１０２）によって待ち状態を繰り返す。メッセージが受信されると、メッセージデータ（入力データ）をチェック（１０３）し、受信メッセージが登録要求５１か否かを判定する（１０４）。登録要求５１であれば、登録情報要求データ５２を作成し、携帯端末に送信（１０６）した後、次のメッセージの受信を待つ（１０７）。上記最初のメッセージが登録要求５１でなければ、その他の処理１０５を行う。

【００２１】次のメッセージとして暗号鍵Ａで暗号化された登録情報５３を受信すると、上記暗号鍵Ａと対応する秘密暗号鍵を適用して登録情報をで解読、解析（１０８）した後、登録情報確認要求メッセージ５４を作成して、携帯端末に送信（１０９）し、次のメッセージの受信を待つ（１１０）。上記登録情報確認要求メッセージ５４のデータ内容７４には、セキュリティコントローラ１０が受信した登録情報メッセージ５３のデータ内容７７を含む。携帯端末からの登録確認応答５５を受信すると、既に受信済の登録情報をセキュリティ管理データとして登録（１１３）し、登録ＯＫレスポンスを作成して携帯端末に送信する（１１４）送付する。なお、携帯端末側から登録確認応答５５として、登録情報メッセージ５３と同様のデータ内容を持つメッセージを送信させ、破線で示すように、受信登録確認応答メッセージ５５のデータ内容を解読、解析した後、既に受信済の登録情報と比較し（１１２）、一致した場合に登録処理（１１３）し、不一致の場合は、登録情報要求ステップ（１０６）から再実行するようにしてもよい。

【００２２】図６は、紛失した携帯端末の所有者から、例えばプッシュホン（電話機）によって非常時連絡先電話番号をダイヤルし、セキュリティコントローラ１０に情報保護を要求した場合の保護システムの動作手順を示す。ここでは、上記情報保護の要求を受け付けた時点で、紛失携帯端末がＰＨＳシステムと通信可能な状態にあり、セキュリティコントローラ１０が紛失携帯端末のアクセスに成功した場合の動作例を示す。また、図６における動作Ｓ１：１３４～Ｓ５：１３８、および後述する図７における動作Ｓ６：１５８～Ｓ７：１５９を実行するセキュリティコントローラ１０の動作フローチャートを図１０に示し、以下図１０の動作ステップも参照して動作説明する。

【００２３】携帯端末の紛失に気付いた所有者が、電話機１８で非常時連絡先の電話番号をダイヤルすると（動作Ｕ１：１３１）、セキュリティコントローラ１０との間にコネクションが確立する。この場合、発呼時に電話機から発信される呼制御信号が保護要求１２１となる。セキュリティコントローラ１０側では、上記非常時電話番号への着信は、音声応答システムに接続され、最初の自動応答メッセージ（認証確認メッセージ）１２２として、例えば、「登録者ＩＤと＃、それに引き続いてパスワードと＃を押してください」という内容の音声メッセージを出力する（動作Ｓ１：１３４、図１０のステップ１０１～２０５）。所有者は、上記音声メッセージに答えて、数字キーと＃ボタンを用いて、登録者ＩＤとパスワードを入力する（動作Ｕ２：１３２）。これらの入力データは、認証データ１２３として送信される。

【００２４】セキュリティコントローラ１０は、上記認証データ１２３を受信すると、登録者ＩＤと同一のＩＤをもつ登録済のセキュリティ管理データレコードを検索し、受信したパスワードが登録済の認証情報８４と一致するか否かを判定し、情報保護の要求者が登録された人物である事を確認した後、要求確認メッセージ１２４を出力する（動作Ｓ２：１３５、図１０のステップ２０６～２０８）。上記要求確認メッセージ１２４は、例えば、「只今から情報保護動作を開始します。携帯端末が発見できなかった場合、引き続いて、探索動作を続けます。すぐに見つからない場合は、後日、連絡します。連絡先の電話番号と＃ボタンを押して、しばらくお待ちください。」のような内容とする。

【００２５】所有者が、電話番号入力と＃ボタン操作（動作Ｕ３：１３３）行うと、セキュリティコントローラは、ＰＨＳシステムＤＢ１１に対して、セキュリティ管理データレコードで登録されているＰＨＳ電話番号を

指定して、携帯端末検索要求１２７を送信する（動作Ｓ３：１３６、図１０のステップ２０９～２１１）。ＰＨＳシステムＤＢ１１は、上記検索要求（１２７）を受信すると、データベースから該当するＰＨＳ電話番号を持つ携帯端末が位置登録されているかを検索し、その結果を携帯端末検索レスポンス１２８として、セキュリティコントローラ１０に送信する（動作Ｎ１：１３９）。

【００２６】セキュリティコントローラ１０は、目的携帯端末が位置登録されている場合、その携帯端末に、予め登録してあった処理番号８５で情報保護の種類を指定した形で、情報保護命令１２９を送信する（動作Ｓ４：１３７、図１０のステップ２１２～２１４）。上記情報保護命令１２９を受信した携帯端末１４は、情報保護プログラムを実行し、これが完了すると、必要に応じて保護データを伴う保護終了報告１３０をセキュリティコントローラ１０に送信する（動作Ｐ１：１４０）。

【００２７】セキュリティコントローラ１０は、上記保護終了報告１３０を受信すると、退避すべき保護データがなければ直接、もしあれば、これを上記セキュリティ管理データレコードと対応付けて蓄積（退避データ記録）した後、情報保護の終了通知１２６を回答（動作Ｓ５：１３８、図１０のステップ２１５～２０８）し、手続きを終了する。上記情報保護の終了通知１２６は、例えば、「携帯端末の情報の保護を完了しました。」の内容をもつ音声メッセージであり、保護データを回収した場合は、その旨を示す音声メッセージを追加する。

【００２８】尚、上記実施例において、ＰＨＳシステムＤＢに対する携帯端末検索要求動作Ｓ３とその応答動作Ｎ１は、上記携帯端末検索要求１２７に応答して、ＰＨＳシステムＤＢが、目的携帯端末が位置登録されている基地局を見つけ出し、この基地局の識別子と対応関係にある基地局所在地（住所）情報を検索し、例えば、上記基地局所在地を中心としたセル半径でもって目的携帯端末の概略的な現在位置を表し、これを上記携帯端末検索レスポンス１２８によってセキュリティコントローラに通知し、セキュリティコントローラが、上記現在位置情報を検索要求者に通知する場合に有効となる。また、図８で説明するように、携帯端末の所有者が情報保護を要求した時点で携帯端末が通信不能の状態にあった場合に、この端末が無線ネットワークに位置登録したのを検出して、自動的に情報保護命令を発行する場合に有効となる。

【００２９】もし、このような端末所有者への端末位置情報サービスを全く必要としない場合は、ＰＨＳシステムＤＢへの端末検索要求１２７を省略し、目的携帯端末が位置登録されているか否かに無関係に、セキュリティコントローラ１０が、上記動作Ｓ３において目的端末への呼（コネクション）設定を試み、コネクションが設定された場合に動作Ｓ４を実行するようにしてもよい。目的端末が通信不能の状態にあった場合は、セキュリティコントローラ１０が、所定の繰返しパターンで自動的に発呼を繰返すようにすればよい。

【００３０】図７は、図６で示した情報保護の要求を受け付けた時点で、紛失携帯端末を発見できなかった場合の動作例を示す。図７の動作シーケンスで、ＰＨＳシステムＤＢ１１がセキュリティコントローラ１０に携帯端末検索レスポンス１２８を送信するまでの手順は図６と同様である。この場合、セキュリティコントローラ１０から検索要求のあった携帯端末の現在位置確認に失敗した場合、ＰＨＳシステムＤＢ１１側で、上記携帯端末の情報レコードに、セキュリティコントローラ１０で探索中の端末である旨を示すフラグをたてておくとよい。この例では、セキュリティコントローラ１０は、ＰＨＳシステムＤＢ１１から位置確認失敗を示す携帯端末検索レスポンス１２８を受信し、動作Ｓ４：１３７において、所有者に、例えば、「お捜しの携帯端末が見つかりません。引き続いて端末の監視を行いますが、ここで端末捜査と情報保護を打ち切る場合は２＃を、継続する場合１＃を押してください。」の内容をもつ音声メッセージ（常駐確認メッセージ）１５１を送信する（図１０のステップ２１９）。

【００３１】所有者が「２＃」を選択した場合は、セキュリティコントローラ１０は、「これでサービスを終了させて頂きます。」の音声メッセージを出力して（動作Ｓ６：１５８、図１０のステップ２２０、２２１、２２７）、通信を終了する。所有者が「１＃」を選択した場合は、上記動作Ｓ６：１５８で、例えば、「お客様の連絡先電話番号は、ＸＸＸＸＸＸＸＸＸで間違いないでしょうか。宜しければ１＃、電話番号を変更する場合は２＃を押し、再度、電話番号を入力した後、＃を押してください。」の内容の音声メッセージ（連絡先確認メッセージ）１５３を送信する（図１０のステップ２２１、２２２）。所有者が、上記確認メッセージに応答操作（動作Ｕ６：１５７）すると、セキュリティコントローラは、上記応答操作による連絡先レスポンス１５４の内容を解析し、「１＃」の場合は、例えば、「これでサービスを終了させて頂きます。」の内容をもつ終了メッセージ１５５を送信した後、通信を終了する。もし、上記確認メッセージに応答して「２＃」と電話番号が入力された場合は、再度、電話番号確認メッセージを送信した後、同様の動作を繰り返す（動作Ｓ７：１５９、図１０のステップ２２３～２２７）

図８は、紛失した携帯端末を自動的に見つけ出すための常駐保護処理の動作手順を示す。また、図１１に、上記図８中の動作Ｓ８：１６６とＳ９：１６７と対応するセキュリティコントローラ１０の動作フローチャートを示し、以下図１１も参照して動作説明する。紛失した携帯端末１４の電源がＯＮになると、内蔵ＰＨＳ電話機能によって、基地局に位置登録要求１６１が発信され、ＰＨＳシステムＤＢ１１が端末の位置登録（動作：１６８）

を行う。ＰＨＳシステムＤＢ１１は、何れかの基地局から位置登録情報１６１を受信すると、位置登録の動作過程で、上記携帯端末の情報レコード中に、セキュリティコントローラ１０で探索中の端末である旨を示すフラグを見つけ、セキュリティコントローラ１０に対して、紛失端末位置を示す位置登録通知１６２を送信する。

【００３２】セキュリティコントローラ１０は、ＰＨＳシステムＤＢからの位置登録通知の受信待ち状態（図１１のステップ１０１）にあり、上記位置登録通知１６２を受信すると、紛失携帯端末１４に対して、ＰＨＳ電話システムによる通信を開始し、情報保護命令１２９を送信する（動作Ｓ８：１６６、図１１のステップ２４３～２４５）。携帯端末１４は、上記情報保護命令１２９に応答して、図６で示したのと同様に情報保護プログラムを実行し、保護終了報告１３０をセキュリティコントローラ１０に送信する。セキュリティコントローラ１０は、上記保護終了報告１３０を受信すると、動作Ｓ９：１６７において、もし、保護データがあればこれを蓄積（避難データ記録し（図１１のステップ２４６～２４８）、セキュリティ管理データレコードに情報保護終了を記録した後、上記データレコードに記憶してある端末所有者の連絡先に自動的ダイヤルし、情報保護の報告１６５を音声メッセージで通知する（図１１のステップ２４９～２５１）。上記実施例では、保護要求のあった携帯端末が位置登録をした時点で、ＰＨＳシステムＤＢ１４が、情報保護要求の有無をチェックし、自動的にセキュリティコントローラに通知する方式となっているが、ＰＨＳシステムＤＢ１４にこのような特殊な機能を付加したくない場合は、セキュリティコントローラ１０が、定期的に携帯端末に発呼を繰り返すことによって、動作８：１６６の切っ掛けを得るようにすればよい。

【００３３】図９は、上述した情報保護動作の実行時に携帯端末、セキュリティコントローラ、ＰＨＳシステムデータベース間で通信するメッセージ７０のフォーマットの一例を示す。メッセージフォーマット７０の基本構造は、図３に示したものと同様で、データ内容７４がメッセージ種類によって異なっている。３０１は、図６及び図７で示した携帯端末検索要求メッセージ１２７のデータ内容を示す。処理命令メッセージ３０５と携帯端末電話番号７９の２つのフィールドからなり、上記処理命令メッセージ３０５には、ＰＨＳシステムＤＢ１１に対する要求内容を示す文字列が設定され、携帯端末電話番号７９には、検索対象となる携帯端末のＰＨＳ電話番号が設定される。

【００３４】３０２は、図６及び図７で示した携帯端末検索レスポンス１２８と、図８で示した位置登録通知１６２に用いるメッセージのデータ内容７４を示す。データ内容は、携帯端末の有無３１０、携帯端末電話番号８２、位置情報３０６の３つのフィールドからなり、携帯端末電話番号８２には、検索対象となった携帯端末のＰＨＳ電話番号が設定され、位置情報３０６には、上記携帯端末が位置するＰＨＳシステム内の接続ポイント（基地局）を示す位置情報が設定され、この位置情報によって、携帯端末の概略的な現在位置を知ることができる。

【００３５】３０３は、図６および図８で示した情報保護命令１２９のメッセージにおけるデータ内容７４を示し、携帯端末識別ＩＤ８１、携帯端末電話番号８２、登録者ＩＤ８３、認証情報８４、処理命令３１１および暗号鍵Ｃ：３０７を含む。携帯端末識別ＩＤ８１、携帯端末電話番号８２、登録者ＩＤ８３、認証情報８４、処理番号８５は、セキュリティ管理データとして登録されたものであり、情報保護命令１２９を受信した時、携帯端末１４側で、受信メッセージの信頼性をチェックするために利用される。暗号鍵Ｃ３０７は、公開暗号鍵方式の公開暗号鍵であり、携帯端末は、この暗号鍵Ｃを用いてセキュリティコントローラに送信する保護情報を暗号化する。

【００３６】３０４は、図６及び図８に示した保護終了報告１３０のメッセージにおけるデータ内容７４を示し、メッセージ種別ＩＤ３０８とデータ３０９の２つのフィールドからなる。メッセージ種別ＩＤ３０８は、これに続くデータフィールド３０９に、例えば、保護終了報告コードのみを含む場合は「０」、保護終了報告コードと保護データとを含み上記保護データに続きがない場合には「１」、保護データに続きデータがある場合は「２」が設定される。データフィールド３０９に内容は、暗号鍵Ｃ３０７を用いて暗号化されている。

【００３７】図１２は、図６、図７、図８における動作Ｎ１：１３９、Ｎ２：１６８を実行するＰＨＳシステムＤＢの動作フローチャートを示す。ＰＨＳシステムＤＢ１１は、受信メッセージをチェックし（ステップ２６１）、受信メッセージが携帯端末からの位置登録要求であれば、動作Ｎ２：１６８を実行する。この場合、通常の位置登録動作を行い（ステップ２７１）、もし、その携帯端末についてセキュリティーコントローラから探索要求がなされいることが判明すると、セキュリティコントローラ宛の通知情報（図８の位置通知１６２）を作成し（２７２）、セキュリティコントローラへ送信（２７３）した後、メッセージ受信待ち状態に戻る。

【００３８】セキュリティコントローラから携帯端末検索要求１２７を受信した場合は、動作Ｎ１：１３９を実行する。この場合、先ず、携帯端末検索要求を解析し（２６４）、検索要求で指定されている携帯端末電話番号（図９に示されている携帯端末電話番号７９）に基づいてデータベース情報を検索し（２６５）、目的端末が位置登録されているか否かをチェックする（２６６）。目的端末が位置登録されていた場合は、図９に示したデータ内容フォーマット３０２におけるフィールド３１０に携帯端末有りを示す「１」、フィールド８２に目的携帯端末の電話番号、フィールド３０６に上記目的携帯端

末を収容している基地局情報が設定された応答メッセージ１２８を作成し（２６７）、セキュリティコントローラに送信する（２７０）。目的携帯端末の位置が未登録の場合、上記フィールド３１０と３０６の「0」が設定された応答メッセージ１２８を作成し（２６８）、これをセキュリティコントローラに送信する（２７０）。

【００３９】図１３は、本発明が適用される携帯端末におけるデータ保護動作Ｐの詳細を示す１フローチャートである。携帯端末は、通常のデータ処理動作状態２８２において通信制御部から割り込みを受けた場合（２８１）、携帯端末のＲＯＭに格納されているデータ保護に専用ソフトウェアを起動し、通信メッセージを解析する（２８４）。ＰＨＳ電話機能および通信制御部が受信待ち状態にあり、ＣＰＵ本体部の電源が未投入状態にある場合は、ＣＰＵ電源を自動的に投入した後、上記通信メッセージの解析を行う。

【００４０】上記割込み原因となった通信制御部での受信メッセージがセキュリティコントローラからの情報保護命令１２９であれば、図３で説明したように、データ部が暗号鍵Ｂ：８６で暗号化されているため、その場合は、暗号鍵Ｂに対応して予めＲＯＭに記憶されている秘密鍵を用いてメッセージ内容を解読する。上記通信内容が情報保護命令１２９でなければ（２８４）、通常の通信処理（２８２）を行い、情報保護命令の場合は、認証チェックを行う（２８６）。認証チェックは、上記情報保護命令中に含まれる認証情報（図９におけるフィールド８５の内容）と、携帯端末情報保護の登録時に携帯端末内に記憶しておいた正当な所有者の認証情報（パスワード）とを比較することによって行う。認証結果に問題があれば以降の処理を省略して最初のステップ２８１へ戻る。

【００４１】認証に問題がなければ、保護命令の内容を解析し（２８７）、処理番号フィールド８５の値からデータ転送の要否を判定し（２８８）、データ転送の必要がなければステップ２９１へ進む。データ転送の必要があれば、情報保護命令中の暗号鍵（暗号鍵Ｃ：３０７）を用いて端末情報（保護データ）を暗号化し（２８９）、暗号化された端末情報をセキュリティコントローラへ送信（２９０）した後、ステップ２９１に進む。ステップ２９１では、端末情報の機密保護（無効化または書き換え）処理を行う（２９１）。データ機密保護は、例えば、端末情報のメモリ消去、または偽データへの変換によって達成する。データ機密保護が終了すると、データ保護終了メッセージをセキュリティコントローラへ送信し（２９２）、割り込み処理を終了し、元の状態に戻る。

【００４２】図１４は、セキュリティコントローラ１０の構成を示す。セキュリティコントローラ１０は、ＣＰＵ２０、ＲＯＭ２１、ＲＡＭ２２、データファイル２３、通信制御部２４、ＰＨＳシステムＤＢとの通信インタフェース２５、携帯端末との通信インタフェース２６、音声応答機能をもつ音声制御部２７、電話インタフェース２８、および内部バス２９からなる。ＣＰＵ２０は、ＲＯＭ２１に用意された制御プログラムに従って、通信制御部２４および音声制御部２７を制御し、通信インタフェース２５を介してＰＨＳシステムＤＢと、通信インタフェース２６を介して携帯情報端末と、電話インタフェース２８を介して電話機と通信する。ＲＡＭ２２は、プログラムのワークエリアとして利用され、ＰＨＳシステムＤＢあるいは携帯端末所有者からのデータの一時保存に利用される。ファイル装置２３は、セキュリティ管理データレコード、紛失端末からの回収データ、あるいは常駐による保護処理動作に必要な情報等の保存に利用される。

【００４３】図１５は、携帯端末１４の構成を示すブロック図である。本発明を適用する携帯端末１４は、ＣＰＵ３１、ＲＯＭ３２、ＲＡＭ３３Ａおよび３３Ｂ、補助記憶装置３４、表示装置（例えば、液晶ディスプレイ）３５、入力装置３６、電源制御部３７、通信インタフェース３８、通信制御部３９、バス４０、電源制御線４１、通信割り込み制御線４２からなる。ＣＰＵ３１は、バス４０を介して、ＲＯＭ３２、ＲＡＭ３３Ａ、３３Ｂ、補助記憶装置３４、表示装置３５、入力装置３６、通信インタフェース３８との間でデータを送受信する。また、電源制御部３７は、電源制御線４１を介して、上記各要素の電源オン、オフを制御する。通信制御部３９は、本実施例では、ＰＨＳ無線通信を実現するための機能として、例えば、アンテナ、高周波回路、ＰＨＳの通信手順制御および通信内容チェック手段を備え、通常のＰＨＳ通信では、通信インタフェース３８を介してＣＰＵ３１と通信メッセージデータのやり取りを行い、通信割り込み制御信号を発生して、ＣＰＵ３１または電源制御部３７に割り込みをかける。

【００４４】ＲＯＭ３２は、携帯端末としての機能を実現するための各種のソフトウェアと、本発明による端末情報保護を実施するための専用ソフトウェア及び制御情報が格納される。ＲＡＭ３３Ａおよび３３Ｂは、電源でバックアップされており、ＲＡＭ３３Ａは、情報保護を必要としない通常のデータ格納用として、また、ＲＡＭ３３Ｂは、本発明を適用して保護すべき特定ファイルデータの格納用として用いられる。上記携帯端末のＣＰＵは、通信制御部からの割込みを受けると、ＲＯＭ３２に用意された専用ソフトウエアを実行し、上記割込みが端末情報保護命令の受信によるものであれば、ＲＡＭ３３Ｂ内の蓄積情報を保護対象として、前述のデータ回収および保護処理を実行する。

【００４５】上記実施例では、各端末で保護対象となる情報を特定のメモリに蓄積しておき、端末紛失時に上記特定メモリ内の全情報に対して情報保護動作がかかるようにしたが、情報保護はデータファイル名を特定して行

うようにしてもよい。例えば、各携帯端末において、保護対象となる情報を特定のファイル名、または特定の頭文字をもつファイル名で管理しておき、情報保護の登録要求時に、端末所有者が保護対象とすべきファイル名（または頭文字等のファイル識別情報）を指定して、これを上記専用ソフトウエアが記憶しておき、情報保護命令が発生した時、上記特定ファイル名のファイルに対して保護処理を実行するようにしてもよい。

【００４６】また、実施例では、端末所有者が電話機を介してセキュリティコントローラと直接交信し、セキュリティコントローラ側が音声応答機能によって情報保護要求を受付制御するようにしたが、紛失端末の所有者がテキストデータの送受信機能を備えた他の無線端末、またはネットワーク５に接続された他の端末からセキュリティコントローラにアクセスし、端末情報保護に必要な情報をデータメッセージ形式で交信するようにしてもよい。また、紛失端末の所有者が普通の電話機で通報した情報保護要求をセキュリティシステム側で係員が受付け、端末所有者が指定した登録者ＩＤに基づいて係員が専用端末からセキュリティコントローラにアクセスし、所有者の認証に必要なパスワード等のデータを係員端末から入力することによって、情報保護を実行するようにしてもよい。

【００４７】

【発明の効果】以上の説明から明らかなように、本発明によれば、携帯端末の通常の使用時において、ファイルアクセス権限確認のためのパスワード入力等の面倒な操作を強制することなく、携帯端末紛失時に端末情報の保護あるいは情報回収が可能となる。また、情報保護要求時に、無線ネットワークにおける端末位置登録機能を利用すれば、紛失端末の概略的な現在位置を知ることができるため、この位置情報に基づいて紛失端末の回収にも役立つことができる。

【図面の簡単な説明】

【図１】本発明による携帯端末情報保護を実現するネットワークシステムの構成図。

【図２】端末情報保護の登録手順の１実施例を示す図。

【図３】上記端末情報保護の登録時に携帯端末とセキュリティコントローラとの間で通信されるメッセージフォーマットの１実施例を示す図。

【図４】上記端末情報保護の登録時に携帯端末に表示される画面の１実施例を示す図。

【図５】上記端末情報保護の登録時にセキュリティコントローラが実行する制御プログラムの処理手順の１実施例を示すフローチャート。

【図６】端末紛失時に実行されるネットワークで実行される情報保護手順の１例を示すシーケンス図。

【図７】端末紛失時に実行されるネットワークで実行される情報保護手順の他の例を示すシーケンス図。

【図８】端末紛失時に実行されるネットワークで実行される情報保護手順のさらに他の例を示すシーケンス図。

【図９】情報保護時に通信されるメッセージフォーマットの１実施例を示す図。

【図１０】情報保護時にセキュリティコントローラが実行する制御プログラムの１実施例を示すフローチャート。

【図１１】情報保護時にセキュリティコントローラが実行する制御プログラムの他の実施例を示すフローチャート。

【図１２】情報保護時にＰＨＳデータベースシステムが実行する制御プログラムの１実施例を示すフローチャート。

【図１３】情報保護時に携帯端末が実行する制御プログラムの１実施例を示すフローチャート。

【図１４】セキュリティコントローラの構成の１例を示すブロック図。

【図１５】携帯端末の構成の１例を示すブロック図。

【符号の説明】

１…無線ネットワークシステム、５…有線網、１０…セキュリティコントローラ、１１…ＰＨＳシステムデータベース、１２…基地局、１４…携帯端末、１８…電話、５１…登録要求、５２…登録情報要求、５３…登録情報、５４…登録情報確認、５５…登録確認応答、５６…登録ＯＫレスポンス、７０…通信メッセージフォーマット、７１…識別ＩＤ、７２…動作ＩＤ、７３…データ量、７４…データ内容、７５…ＣＲＣ、７６…登録要求データ、７７…登録情報データ、７８…登録ＯＫレスポンスデータ、９０…登録開始画面、９１…登録入力画面、９２…所有者確認画面、１２１…保護要求、１２２…認証確認メッセージ、１２３…認証データ、１２４…要求確認メッセージ、１２５…要求送付、１２６…終了通知、１２７…携帯端末検索要求、１２８…携帯端末検索レスポンス、１２９…情報保護命令、１３０…保護終了報告及び保護データ、１５１…常駐確認メッセージ、１５２…常駐レスポンス、１５３…連絡先確認メッセージ、１５４…連絡先レスポンス、１５５…終了メッセージ、３０１…携帯端末検索データ、３０２…携帯端末検索レスポンスデータ、３０３…情報保護命令データ、３０４…保護データ。

【図1】

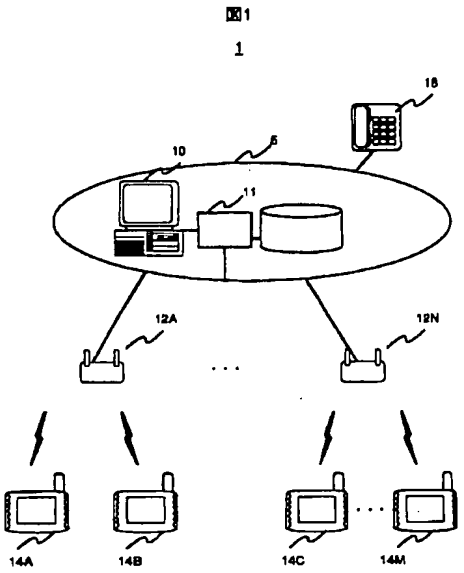


図1
1
18
10
5
11
12A
12N
14A
14B
14C
14M

【図2】

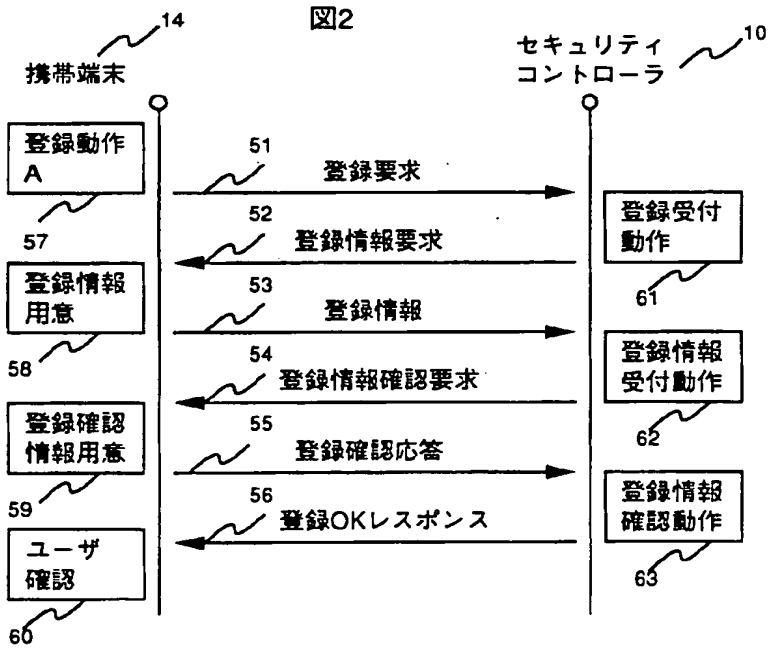
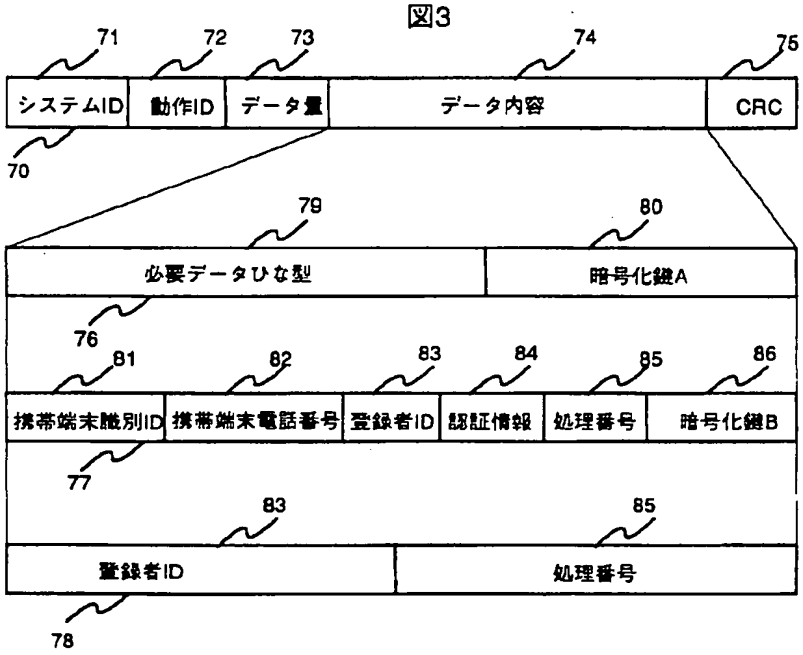


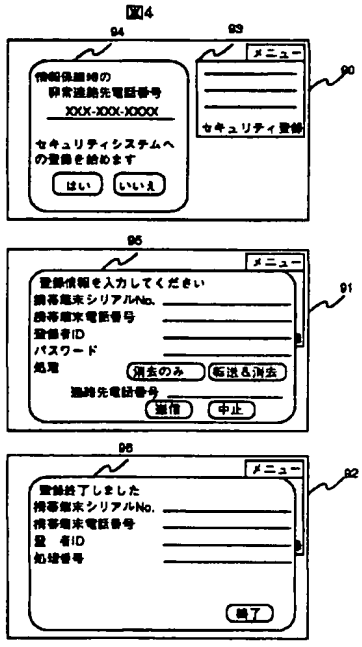
図2
14
携帯端末
セキュリティ
コントローラ
10
登録動作
A
57
登録情報
用意
58
登録確認
情報用意
59
ユーザ
確認
60
51
登録要求
52
登録情報要求
53
登録情報
54
登録情報確認要求
55
登録確認応答
56
登録OKレスポンス
登録受付
動作
61
登録情報
受付動作
62
登録情報
確認動作
63

【図3】

図3

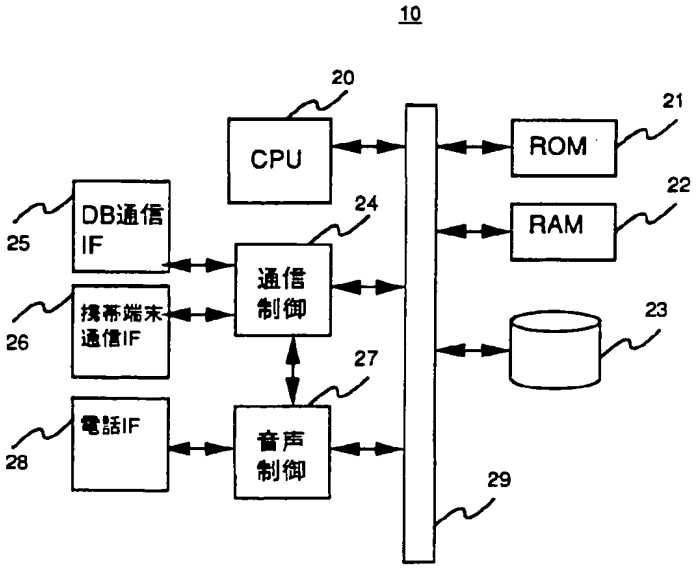


【図4】



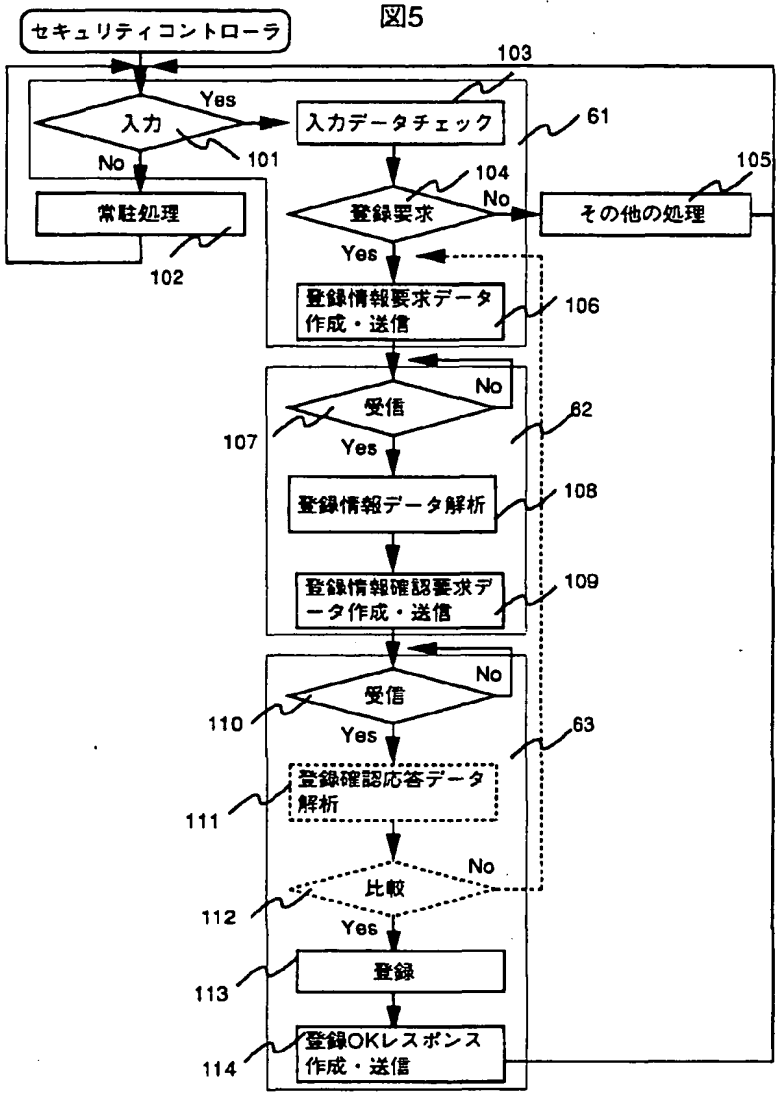
【図14】

図14



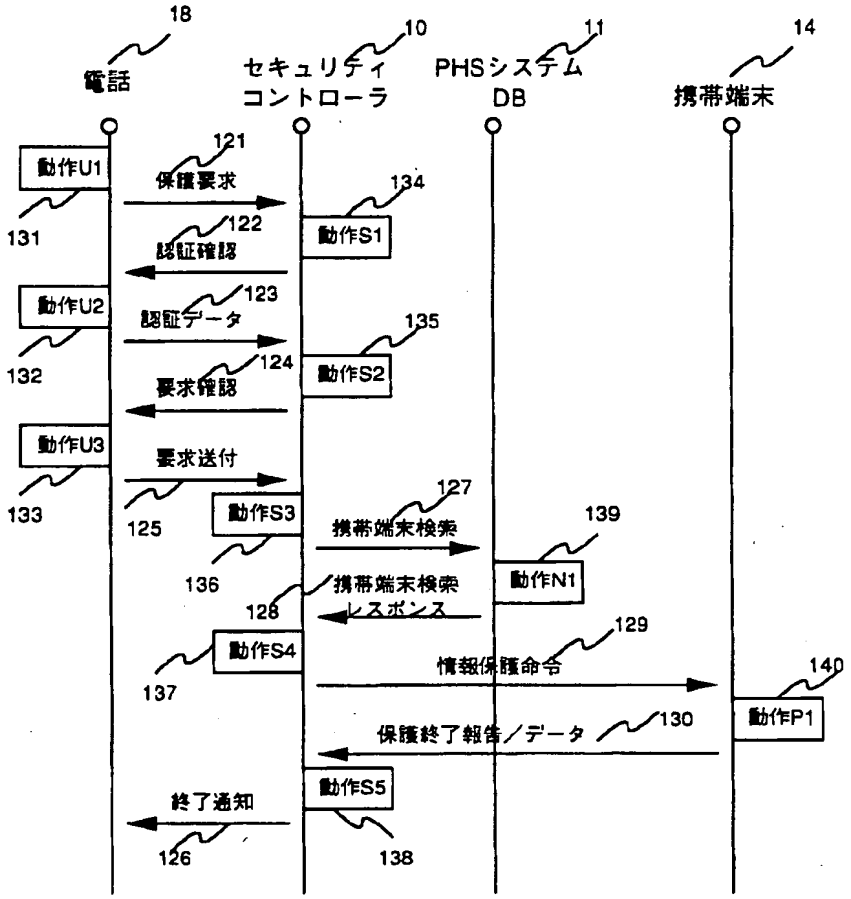
【図5】

図5


セキュリティコントローラ
103
Yes
入力
入力データチェック
61
No
101
104
105
常駐処理
登録要求
No
その他の処理
Yes
102
登録情報要求データ作成・送信
106
No
受信
62
107
Yes
登録情報データ解析
108
登録情報確認要求データ作成・送信
109
No
受信
110
Yes
63
登録確認応答データ解析
111
No
比較
112
Yes
登録
113
登録OKレスポンス作成・送信
114

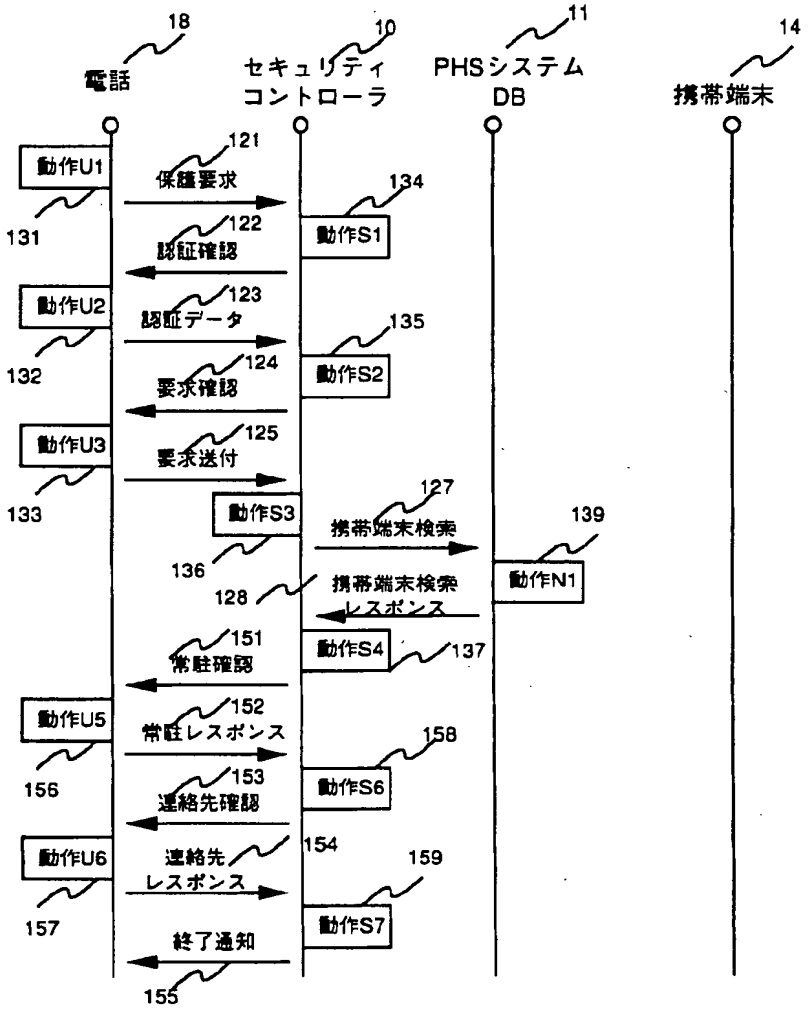
【図6】

図6


18
電話
10
セキュリティ
コントローラ
11
PHSシステム
DB
14
携帯端末
動作U1
131
121
保護要求
134
動作S1
122
認証確認
動作U2
132
123
認証データ
135
動作S2
124
要求確認
動作U3
133
要求送付
125
動作S3
127
携帯端末検索
139
動作N1
136
128
携帯端末検索
レスポンス
動作S4
137
129
情報保護命令
140
動作P1
保護終了報告／データ
130
動作S5
終了通知
126
138

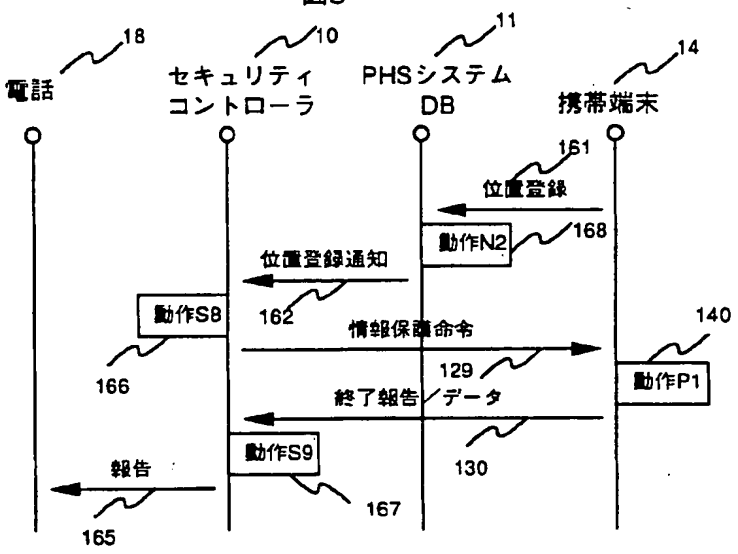
【図7】

図7


18
電話
10
セキュリティ
コントローラ
11
PHSシステム
DB
14
携帯端末
動作U1
131
121
保護要求
134
動作S1
122
認証確認
動作U2
132
123
認証データ
135
動作S2
124
要求確認
動作U3
133
125
要求送付
127
動作S3
携帯端末検索
139
136
動作N1
128
携帯端末検索
レスポンス
151
常駐確認
動作S4
137
動作U5
156
152
常駐レスポンス
158
動作S6
153
連絡先確認
動作U6
157
154
連絡先
レスポンス
159
動作S7
終了通知
155

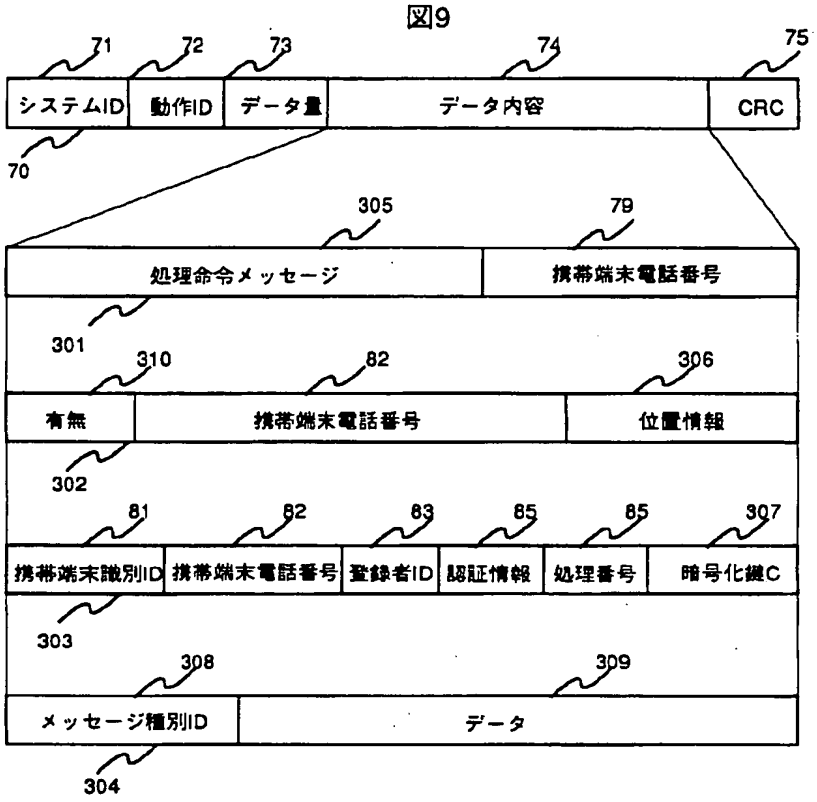
【図８】

図8


電話
18
セキュリティ
コントローラ
10
PHSシステム
DB
11
携帯端末
14
161
位置登録
動作N2
168
位置登録通知
162
動作S8
166
情報保護命令
140
129
データ
動作P1
終了報告
130
動作S9
167
報告
165

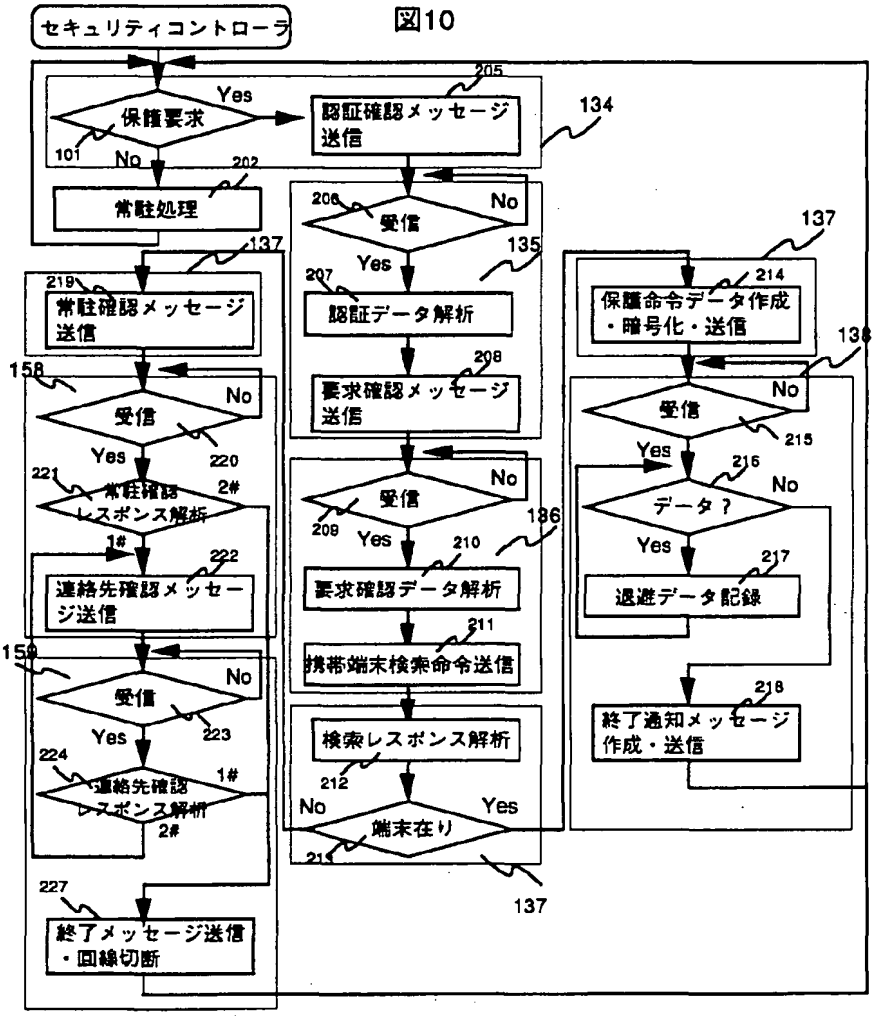
【図9】

図9


71
72
73
74
75
システムID
動作ID
データ量
データ内容
CRC
70
305
79
処理命令メッセージ
携帯端末電話番号
301
310
82
306
有無
携帯端末電話番号
位置情報
302
81
82
83
85
85
307
携帯端末識別ID
携帯端末電話番号
登録者ID
認証情報
処理番号
暗号化鍵C
303
308
309
メッセージ種別ID
データ
304

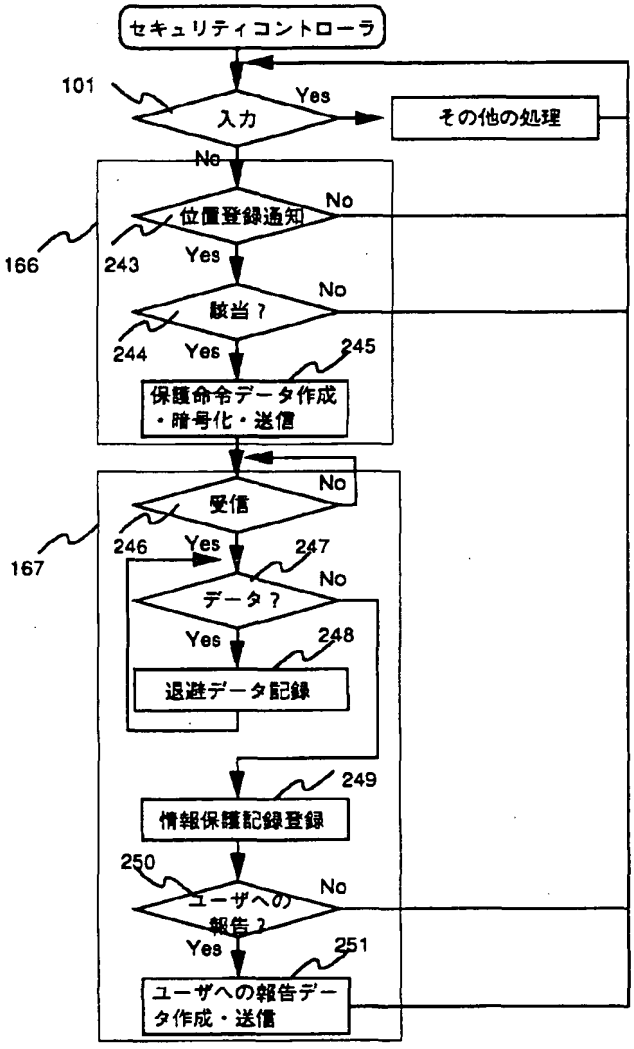
【図１０】

図10


セキュリティコントローラ
保護要求
Yes
No
101
認証確認メッセージ送信
205
134
常駐処理
202
受信
206
No
Yes
135
認証データ解析
207
要求確認メッセージ送信
208
受信
No
Yes
209
要求確認データ解析
210
136
携帯端末検索命令送信
211
検索レスポンス解析
212
No
Yes
端末在り
213
137
137
常駐確認メッセージ送信
219
158
受信
No
Yes
220
常駐確認レスポンス解析
221
2#
1#
連絡先確認メッセージ送信
222
159
受信
No
Yes
223
連絡先確認レスポンス解析
224
1#
2#
227
終了メッセージ送信・回線切断
137
保護命令データ作成・暗号化・送信
214
138
受信
No
Yes
215
データ？
216
No
Yes
退避データ記録
217
終了通知メッセージ作成・送信
218

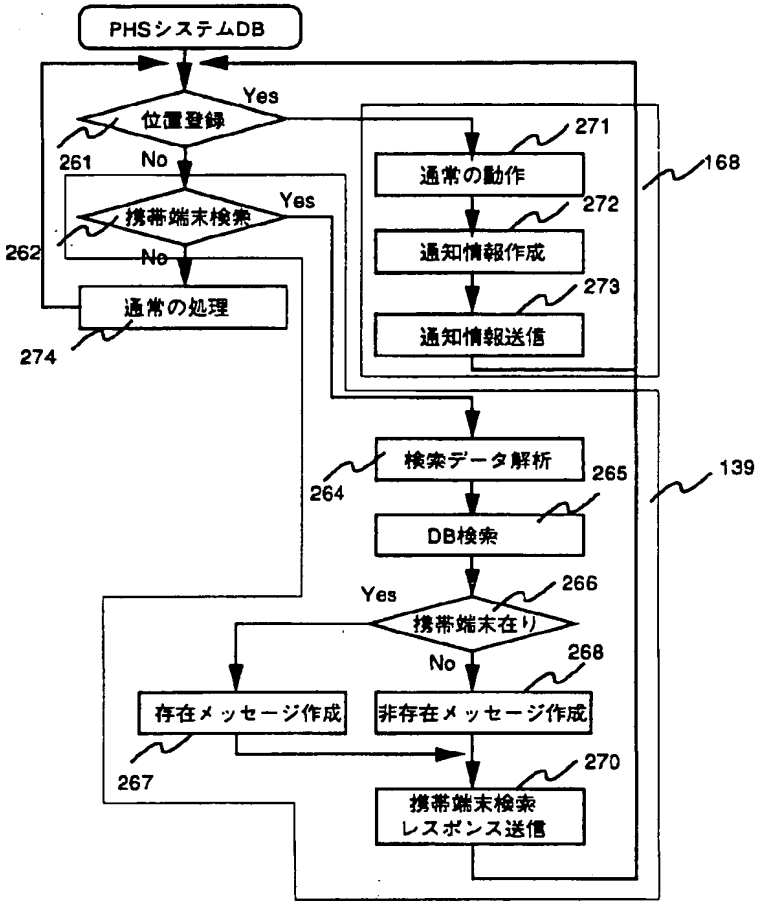
【図１１】

図11


セキュリティコントローラ
101
入力
Yes
その他の処理
No
位置登録通知
No
166
243
Yes
該当？
No
244
Yes
245
保護命令データ作成・暗号化・送信
No
受信
167
246
Yes
247
No
データ？
Yes
248
退避データ記録
249
情報保護記録登録
250
ユーザへの報告？
No
Yes
251
ユーザへの報告データ作成・送信

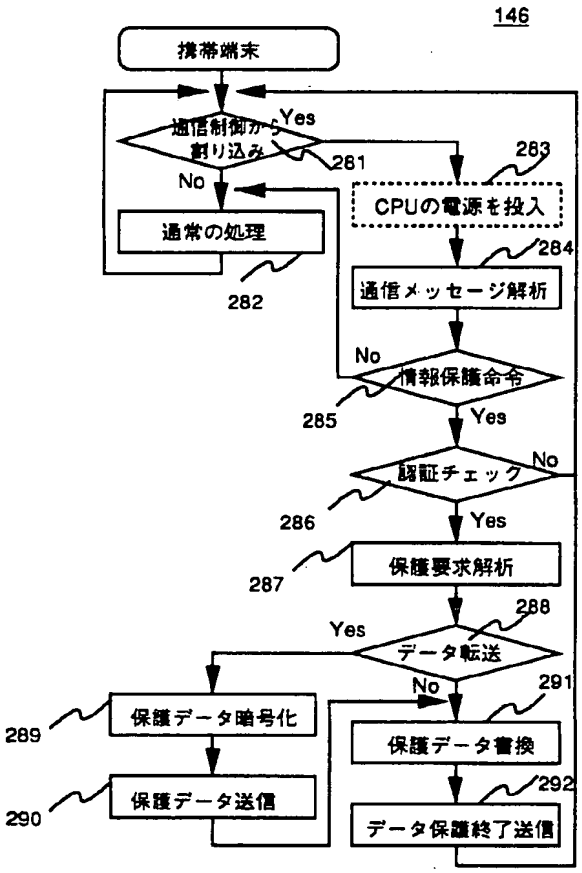
【図１２】

図12


PHSシステムDB
位置登録
Yes
No
261
携帯端末検索
Yes
No
262
通常の処理
274
271
通常の動作
272
通知情報作成
273
通知情報送信
168
検索データ解析
264
265
DB検索
139
Yes
携帯端末在り
266
No
268
存在メッセージ作成
非存在メッセージ作成
267
270
携帯端末検索
レスポンス送信

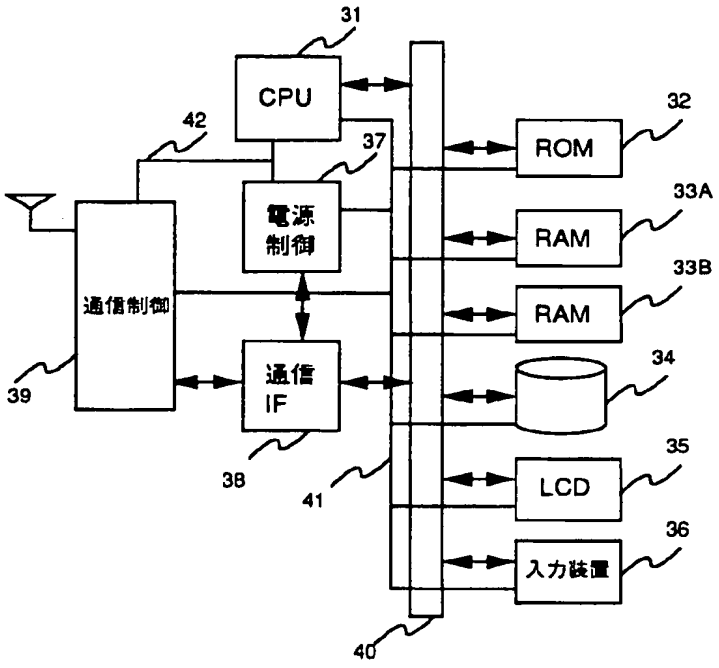
【図１３】

図13


146
携帯端末
通信制御から割り込み
Yes
No
281
283
CPUの電源を投入
284
通信メッセージ解析
通常の処理
282
No
情報保護命令
285
Yes
No
認証チェック
286
Yes
保護要求解析
287
288
Yes
データ転送
No
291
保護データ暗号化
289
保護データ書換
292
保護データ送信
290
データ保護終了送信

【図１５】

図15



フロントページの続き

(51)Int.Cl.6	識別記号	庁内整理番号	FI		技術表示箇所
H04M 11/00	302		H04L 9/00	673A	
			H04Q 7/04	D	